EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

RECORD OF PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 REGULATION 2018/1725[1] NOTIFICATION TO THE DATA PROTECTION OFFICER

NAME OF PROCESSING OPERATION[2]: FRA survey with organisations providing support to persons fleeing Ukraine

Reference number: DPR-2023-181 (to be completed by the DPO)
Creation date of this record: 13/04/2023
Last update of this record: 13/04/2023
Version: 1.0

Part 1 (Publicly available)

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: European Union Agency for Fundamental Rights (FRA) Schwarzenbergplatz 11, A-1040 Vienna, Austria Telephone: +43 1 580 30 – 0 Email: contact@fra.europa.eu Organisational unit **responsible**[4] for the processing activity: Equality, Roma and Social Rights (ERSR) Unit Contact details: SecSocialRights@fra.europa.eu Data Protection Officer (DPO): dpo@fra.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))[5]	
The data is processed by the FRA itself	☒
The data is processed also by a third party (contractor) [mention the third party]	☒
(Specify if they are processors or joint controllers)	

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

2 **Personal data** is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.
Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 In case of more than one controller (e.g. joint FRA research), all controllers need to be listed here

4 This is the unit that decides that the processing takes place and why.

5 Is the FRA itself conducting the processing? Or has a provider been contracted?

The following third parties might be involved in the processing operation as processors:

FRA's Web hosting contractor, Managing Innovation Strategies, SLL (MainStrat) in consortium with SARENET, S.A.U.

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).

Since 24 February 2022, the European Union experiences a mass influx of displaced persons fleeing the war in Ukraine. In response, the European Council activated the 2001 EU Temporary Protection Directive (Council Directive 2001/55/EC) through Council Implementing Decision (EU) 2022/382 of 4 March 2022. The Directive provides minimum standards for giving temporary protection in the event of a mass influx of displaced persons. However, the Directive is implemented for the first time. Therefore information on its implementation on the ground, including experience of local support providing organisations, are of key importance.

The purpose of the processing of respondents' personal data is to complement and update Franet research in support of a FRA research project on local/city measures ensuring access to selected rights for temporary protection beneficiaries. FRANET contractors identified prospective respondents, including their email addresses, in organisations providing support to temporary protection beneficiaries, based on a previous processing activity (DPO-2022-173), who agreed to be contacted to participate in the survey.

The identified respondents have practical experience in supporting temporary protection beneficiaries and are based at the locations in the 12 Member States covered by the research: Austria, Belgium, Czechia, Germany, Estonia, France, Ireland, Italy, Poland, Romania, Sweden, and Slovakia.

FRA would invite the identified respondents by email to participate in an online survey (using Lime Survey tool) on their experiences of challenges and good practices in supporting temporary protection beneficiaries to access housing, education, employment and healthcare (see attached questionnaire).

The data collected though the online survey will be stored in the SQL database on the servers of FRA's webhosting contractor (located Spain) wherefrom they will be exported into a data set. The data set will be securely kept (protected by password).

The data set will analysed by FRA staff in such a manner that responses cannot be identified and linked to the respondents. Their respective organisations will be referred to as "support provider", indicating the thematic field of support (i.e. housing, education, employment or healthcare) and the location concerned. An annex will list the names and locations of the respondents' organisations.

4) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are being processed?

FRA staff ☐

Non-FRA staff, e.g. practitioners working for organisations supporting persons arriving from Ukraine ☒

The survey will collect anonymised (non-identifiable) data from respondents who have practical professional experiences in supporting temporary protection beneficiaries to access housing, education, employment and healthcare at the locations in the 12 Member States covered by the research.

5) Categories of personal data processed (Article 31.1(c))

Please tick all that apply and give details where appropriate

(a) **General personal data (add or delete as appropriate – the data in the brackets are only examples)**

Personal details ☐

Contact details: email address ☒

The email address of the respondent will be stored if the button "Save and resume later" is clicked and if the respondent provides an email address. The email address field is not mandatory. If an email address is provided it will be used to send the user an email with a link to the unsubmitted survey as well as their pseudonym and the redacted password and it will be stored until the respondent completes the survey or until up to 48 hours after the survey deadline has expired.

Education & Training details ☐

Employment details: name and location of employing organisation, thematic area of work ☒

For thematic areas of work, survey respondents are asked to select general categories: housing, education, employment, healthcare, all

Financial details (e.g. financial identification form, bank account information) ☐

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other (please give details):

Two session cookies are used:

1. *PHPSESSID*
   Domain: fra.europa.eu
   This cookie is native to PHP applications. The cookie is used to store and identify a users" unique session ID for the purpose of managing user session on the website. The cookie is a session cookie and is deleted when all the browser windows are closed.

2. *YII_CSRF_TOKEN*
   Domain: fra.europa.eu
   This cookie is created to prevent Cross-Site Request Forgery (CSRF). The cookie is a session cookie and is deleted when all the browser windows are closed.

Also, a first party cookie is collected:

3. *LS_(survy-id)_STATUS*
   A cookie will also be stored on the users device to prevent repeated participation. The first-party cookie is called LS_(survy-id)_STATUS and expires 365 days after the survey has been submitted. This cookie prevents users from the same computer from accessing the survey more than once.

(b) **Special categories of personal data** (Article 10)
The personal data collected reveal:

Racial or ethnic origin ☐

Political opinions ☐

Religious or philosophical beliefs ☐

Trade union membership ☐

Genetic, biometric or data concerning health ☐

Information regarding an individual's sex life or sexual orientation ☐

N/A ☐

(c) **Personal data relating to criminal convictions and offences** (Article 11)

Criminal record (or similar, e.g. declaration of good conduct) ☐

N/A ☐

6) Recipient(s) of the data (Article 31.1 (d))

*Recipients are all parties who have access to the personal data. Who will have access to the data **within** FRA? Who will have access to the data **outside** FRA? No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).*

Designated **FRA** staff members
(please specify which team and Unit-no need to mention specifically the names of colleagues) ☒

The data analysts and statisticians from FRA's team will have access to the dataset. The analysis of the dataset will be done to provide fully anonymised data and results from the survey, leading to FRA publications.

The data set can be accessed by the responsible head of the unit (Equality, Roma & Social Rights Unit) and delegated members of the project team.

Access to the dataset is also given to two FRA staff members from the Communications and events unit who are administrators of the Limesurvey application.

Recipients **outside** FRA:
(please provide a generic/functional mailbox) ☐

7) Transfers to third countries or international organisations (Article 31.1 (e))[6]

If the personal data are transferred outside the European Economic Area or to international organisations, this needs to be specifically mentioned, since it increases the risks of the processing operation.

Transfer outside of the EU or EEA

Yes ☐

No ☒

If yes, specify to which country:

Transfer to international organisation(s)

Yes ☐

No ☒

If yes specify to which organisation:

Legal base for the data transfer

☐ Transfer on the basis of the European Commission's adequacy decision (Article 47)

[6] **Processor** in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards.

☐ Transfer subject to appropriate safeguards (Article 48.2 and .3), specify:

a) ☐ A legally binding and enforceable instrument between public authorities or bodies.

Standard data protection clauses, adopted by

b) ☐ the Commission, or

c) ☐ the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2) .

d) ☐Binding corporate rules, ☐ Codes of conduct , ☐ Certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

Subject to the authorisation from the European Data Protection Supervisor:
☐ Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.

☐ Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

☐ Transfer based on an international agreement (Article 49), specify:

Derogations for specific situations (Article 50.1 (a) –(g))

☐ N /A
☐ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply In the absence of an adequacy decision, or of appropriate safeguards, transfer of personal data to a third country or an international organisation is based on the following condition(s):

☐ (a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
☐ (b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
☐ (c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
☐ (d) The transfer is necessary for important reasons of public interest
☐ (e) The transfer is necessary for the establishment, exercise or defense of legal claims
☐ (f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
☐ (g) The transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case

8) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Please indicate the starting point and differentiate between categories of persons or data where needed (e.g. in selection procedures candidates who made it onto the reserve list vs. those who didn`t). Are the data limited according to the adage "as long as necessary, as short as possible"?

Data collected will be anonymised i.e. any metadata that could possibly identify an individual will be deleted. The anonymised dataset will be stored indefinitely by FRA. The anonymised dataset may be indefinitely stored also by a data service (such as e.g. Gesis).

The email address of the respondent will be stored if the button "Resume later" is clicked and if the respondent provides an email address. The email address field is not mandatory. If an email address is provided it will be used to send the user an email with a link to the unsubmitted survey as well as their pseudonym and the redacted password, and it will be stored until the respondent completes the survey or until up to 48 hours after the survey deadline has expired.

9) Technical and organisational security measures (Article 31.1(g))

Please specify where/how the data are stored during and after the processing; please describe the security measures taken by FRA or by the contractor

How is the data stored?

Document Management System (DMS) ☒

FRA network shared drive ☐

Outlook Folder(s) ☐

CRM ☐

Hardcopy file ☐

Cloud (Microsoft Office 365, please see data protection notice here) ☒

External contractor under the provisions of a framework contract ☒
FRA undertakes to ensure security updates to the software and hosting environment take place in a timely manner.

The hosting consortium has security policies in place to ensure the physical and logical security for the infrastructure it operates. The consortium has also performed a security self-assessment to demonstrate the compliance of its Data Centre with the security requirements outlined by the ISO 27001 standard.
Added to this, the following sub-sections show the specific security measures at three levels:
1. FRA Platform environment, by means of 2 Fortinet firewalls.
2. FRA Applications, by means of Frontal Pro Web Application Firewall.
3. Physical security in the Data Center.

10) Exercising the rights of the data subject (Article 14 (2))
How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react?
See further details in the Data Protection notice: e-mail to TPDlocalauthorities@fra.europa.eu ***Data subject rights*** ☒ Right of access ☒ Right to rectification ☒ Right to erasure (right to be forgotten) ☒ Right to restriction of processing ☐ Right to data portability ☒ Right to object ☒ Notification obligation regarding rectification or erasure of personal data or restriction of processing ☒ Right to have recourse ☒ Right to withdraw consent at any time

Part 2 – Compliance check and risk screening (internal)

11) Lawfulness of the processing (Article 5(a)–(e))[7]: Processing necessary for:

[7] Tick (at least) one and explain why the processing is necessary for it. Examples:

(a) a task attributed to your EUI by legislation, e.g. procedures under the staff regulations or tasks assigned by an Agency's founding regulation. Please mention the specific legal basis (e.g. "Staff Regulations Article X, as implemented by EUI IR Article Y", instead of just "Staff Regulations")

(a2) not all processing operations required for the functioning of the EUIs are explicitly mandated by legislation; recital 17 explains that they are nonetheless covered here, e.g. internal staff directory, access control.

(b) a specific legal obligation to process personal data, e.g. obligation to publish declarations of interest in an EU agency's founding regulation.

(c) this is rarely used by the EUIs.